AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for ~~to facilitate secure messaging~~enabling a database system to prove that an origin system sent a message, comprising:

~~creating a message at an origin;~~

~~computing a digest of the message;~~

~~signing the digest using an origin private encryption key;~~

~~sending the message and the digest to a queue located in a third party device for delivery to a recipient;~~

receiving the message and ~~the~~ a signed first digest ~~at the queue~~of the message at a database system from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key;

using an origin public encryption key that is associated with the origin private encryption key to verify~~ing~~ that the signed first digest was signed ~~at~~ by the origin system, thereby proving that the origin system created and sent the message~~by using an origin public encryption key, whereby the origin cannot deny creating the message~~; and

persistently storing the signed first digest with the message, thereby enabling the database system to present the signed first digest as proof that the origin system sent the message.

~~if the digest is verified as being signed at the origin,~~

~~placing the message and digest on the queue and persistently storing a record of this transaction, and notifying the recipient that the message is available;~~

~~generating a request at the recipient to receive the message from the queue located in the third party device;~~

~~creating a signature for the request using a recipient private encryption key;~~

~~sending the request and the signature to the queue;~~

~~validating the request at the queue using the signature and a recipient public encryption key; and~~

~~if the request is valid,~~

~~dequeueing the message from the queue,~~

~~sending the digest to the recipient;~~

~~signing the digest at the recipient using the recipient private encryption key creating a signed digest;~~

~~returning the signed digest to the queue,~~

~~validating the signed digest at the queue using the recipient public encryption key, whereby the recipient cannot deny requesting to receive the message, and~~

~~if the signed digest is valid, persistently storing a record of this transaction and sending the message to the recipient.~~

2. (Canceled).

3. (Currently amended) The method of claim 22 ~~claim 1~~, further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

4. (Original) The method of claim 3, further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

5. (Previously presented) The method of claim 1, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

6. (Currently amended) The method of claim 22 ~~claim 1~~, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

7. (Previously presented) The method of claim 1, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

8. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method ~~to facilitate secure messaging~~ for enabling a database system to prove that an origin system sent a message, the method comprising:

~~creating a message at an origin;~~

~~computing a digest of the message;~~

~~signing the digest using an origin private encryption key;~~

~~sending the message and the digest to a queue located in a third party device for delivery to a recipient;~~

receiving the message and ~~the~~ a signed first digest ~~at the queue~~of the message at a database system from the origin system, wherein the signed first

digest was created by signing a digest of the message using an origin private encryption key;

using an origin public encryption key that is associated with the origin private encryption key to verify~~ing~~ that the signed first digest was signed ~~at~~ by the origin system, thereby proving that the origin system created and sent the message~~by using an origin public encryption key, whereby the origin cannot deny creating the message~~; and

persistently storing the signed first digest with the message, thereby enabling the database system to present the signed first digest as proof that the origin system sent the message.

~~if the digest is verified as being signed at the origin,~~

~~placing the message and digest on the queue and persistently storing a record of this transaction, and~~

~~notifying the recipient that the message is available;~~

~~generating a request at the recipient to receive the message from the queue located in the third party device;~~

~~creating a signature for the request using a recipient private encryption key;~~

~~sending the request and the signature to the queue;~~

~~validating the request at the queue using the signature and a recipient public encryption key; and~~

~~if the request is valid,~~

~~dequeueing the message from the queue,~~

~~sending the digest to the recipient,~~

~~signing the digest at the recipient using the recipient private encryption key creating a signed digest,~~

~~returning the signed digest to the queue,~~

~~validating the signed digest at the queue using the recipient public encryption key, whereby the recipient cannot deny requesting to receive the message, and~~

~~if the signed digest is valid, persistently storing a record of this transaction and sending the message to the recipient.~~

9. (Canceled).

10. (Currently amended) The computer-readable storage medium of claim 23 ~~claim 8~~, the method further comprising passing the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

11. (Original) The computer-readable storage medium of claim 10, the method further comprising passing the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

12. (Previously presented) The computer-readable storage medium of claim 8, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

13. (Currently amended) The computer-readable storage medium of claim 23 ~~claim 8~~, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

14. (Previously presented) The computer-readable storage medium of claim 8, wherein computing the digest includes using one of message digest 2

(MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

15. (Currently amended) An apparatus for~~to facilitate secure messaging~~ enabling a database system to prove that an origin system sent a message, comprising:

~~a first creating mechanism that is configured to create a message at an origin;~~

~~a computing mechanism that is configured to compute a digest of the message;~~

~~a first signing mechanism that is configured to sign the digest using an origin private encryption key;~~

~~a first sending mechanism that is configured to send the message and the digest to a queue located in a third party device for delivery to a recipient;~~

a first receiving mechanism that is configured to receive the message and ~~the~~ a signed first digest ~~at the queue~~of the message at a database system from the origin system, wherein the signed first digest was created by signing a digest of the message using an origin private encryption key;

a first verifying mechanism that is configured to use an origin public encryption key that is associated with the origin private encryption key to verify that the signed first digest was signed ~~at~~ by the origin system, thereby proving that the origin system created and sent the message~~by using an origin public encryption key, whereby the origin cannot deny creating the message~~; and

a first storing~~placing~~ mechanism that is configured to ~~place~~ persistently store the signed first digest with the message, thereby enabling the database system to present the signed first digest as proof that the origin system sent the message. ~~the message and digest on the queue and persistently store a record of~~

~~this transaction; a notifying mechanism that is configured to notify the recipient that the message is available;~~

~~a generating mechanism that is configured to generate a request at the recipient to receive the message from the queue located in the third party device;~~

~~a second creating mechanism that is configured to create a signature for the request using a recipient private encryption key;~~

~~a second sending mechanism that is configured to send the request and the signature to the queue;~~

~~a first validating mechanism that is configured to validate the request at the queue using the signature and a recipient public encryption key;~~

~~a dequeueing mechanism that is configured to dequeue the message from the queue;~~

~~a third sending mechanism that is configured to send the digest to the recipient;~~

~~a second signing mechanism that is configured to sign the digest at the recipient using the recipient private encryption key creating a signed digest;~~

~~a returning mechanism that is configured to return the signed digest to the queue;~~

~~a second validating mechanism that is configured to validate the signed digest at the queue using the recipient public encryption key and persistently store a record of this transaction, whereby the recipient cannot deny requesting to receive the message; and~~

~~wherein the third sending mechanism is further configured to send the message to the recipient.~~

16. (Canceled).

17. (Currently amended) The apparatus of claim 24 ~~claim 15~~, further comprising a passing mechanism that is configured to pass the message and the digest through a plurality of queues between the origin and the recipient, whereby the recipient and the origin are subscribers of different queues.

18. (Original) The apparatus of claim 17, wherein the passing mechanism is further configured to pass the message and the digest through a plurality of databases, wherein each database in the plurality of databases includes at least one queue of the plurality of queues.

19. (Previously presented) The apparatus of claim 15, wherein the origin public encryption key and the origin private encryption key are a key pair of a public key encryption system.

20. (Currently amended) The apparatus of claim 24 ~~claim 15~~, wherein the recipient public encryption key and the recipient private encryption key are a key pair of a public key encryption system.

21. (Previously presented) The apparatus of claim 15, wherein computing the digest includes using one of message digest 2 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm 1 (SHA1).

22. (New) The method of claim 1, further comprising:

receiving a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

validating the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

sending a second digest of the message to the recipient system;

receiving a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

validating the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

persistently storing the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.

23. (New) The computer-readable storage medium of claim 8, the method further comprising:

receiving a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

validating the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

sending a second digest of the message to the recipient system;

receiving a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

validating the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

persistently storing the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.

24. (New) The apparatus of claim 15, further comprising:

a second receiving mechanism configured to receive a signed receive-request from a recipient system for receiving the message, wherein the receive-request is signed using a recipient private encryption key;

a second validating mechanism configured to validate the signed receive-request using a recipient public encryption key that is associated with the recipient private encryption key;

a second sending mechanism configured to send a second digest of the message to the recipient system;

a third receiving mechanism configured to receive a signed second digest from the recipient system, wherein the signed second digest was created by signing the second digest using the recipient private encryption key;

a third validating mechanism configured to validate the signed second digest using the recipient public encryption key, thereby proving that the recipient system requested to receive the message; and

a second storing mechanism configured to persistently store the signed second digest, thereby enabling the database system to present the signed second digest as proof that the recipient system requested to receive the message.